O I P E
JC37
OCT 2 9 2003
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANTS : A-Jung Kim et al.
SERIAL NO. : 10/677,461
FILED : October 2, 2003
FOR : METHOD OF TRANSMITTING SECURITY DATA IN AN ETHERNET PASSIVE OPTICAL NETWORK SYSTEM

PETITION FOR GRANT OF PRIORITY UNDER 35 USC 119

MAIL STOP PATENT APPLICATION
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA. 22313-1450

Dear Sir:

Applicant hereby petitions for grant of priority of the present Application on the basis of the following prior filed foreign Application:

COUNTRY	SERIAL NO.	FILING DATE
Republic of Korea	2002-60176	October 2, 2002

To perfect Applicant's claim to priority, a certified copy of the above listed prior filed Application is enclosed. Acknowledgment of Applicant's perfection of claim to priority is accordingly requested.

Respectfully submitted,

Steve S. Cha
Attorney for Applicant
Registration No. 44,069

CHA & REITER
411 Hackensack Ave, 9th floor
Hackensack, NJ 07601
(201)518-5518

Date: October 24, 2003

Certificate of Mailing Under 37 CFR 1.8

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to MS PATENT APPLICATION (PRIORITY DOCUMENT, COMMISSIONER FOR PATENTS, P. O. BOX 1450, ALEXANDRIA, VA. 22313-1450 on October 24, 2003.

Steve S. Cha, Reg. No. 44,069
Name of Registered Rep.)

10/24/03
(Signature and Date)

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원번호 : 10-2002-0060176
Application Number

출원년월일 : 2002년 10월 02일
Date of Application OCT 02, 2002

출원인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 09 월 25 일

특허청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0007
【제출일자】	2002.10.02
【국제특허분류】	H04J
【발명의 명칭】	트리 구조 네트워크 상에서의 인증과 프라이버시 보장을 위한 전송 방법
【발명의 영문명칭】	TRANSMITTING METHOD FOR AUTHENTICATION AND PRIVACY SECURITY ON TREE STRUCTURE NETWORK
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이건주
【대리인코드】	9-1998-000339-8
【포괄위임등록번호】	1999-006038-0
【발명자】	
【성명의 국문표기】	김아정
【성명의 영문표기】	KIM,A JUNG
【주민등록번호】	660121-2037322
【우편번호】	140-731
【주소】	서울특별시 용산구 이태원2동 청화아파트 5동 805
【국적】	KR
【발명자】	
【성명의 국문표기】	김진희
【성명의 영문표기】	KIM,Jin Hee
【주소】	경기도 수원시 팔달구 영통동 963-2 쌍용 아파트 544-707
【국적】	US
【발명자】	
【성명의 국문표기】	임세윤
【성명의 영문표기】	LIM,Se Youn
【주민등록번호】	730815-1094428

【우편번호】	151-802
【주소】	서울특별시 관악구 남현동 1054-33 신원빌리지 302호
【국적】	KR
【발명자】	
【성명의 국문표기】	송재연
【성명의 영문표기】	SONG,Jae Youn
【주민등록번호】	720523-2178211
【우편번호】	463-020
【주소】	경기도 성남시 분당구 수내동 양지마을 한양아파트 514동 902호
【국적】	KR
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이건주 (인)

【수수료】				
【기본출원료】	20	면	29,000	원
【가산출원료】	3	면	3,000	원
【우선권주장료】	0	건	0	원
【심사청구료】	0	항	0	원
【합계】	32,000	원		

【요약서】

【요약】

가. 발명이 속하는 기술분야

본 발명은 점대다점 구조를 가지는 트리 구조 네트워크 상에서의 보안을 위한 전송 방법에 관한 것이다.

나. 발명이 해결하고자 하는 기술적 과제

본 발명의 목적은 점대다점의 트리 구조를 가지는 네트워크, 특히 이더넷 수동 광가입자망에서 보안을 위한 인증과정과 데이터의 암호화를 포함하는 전송 방법을 제공함에 있다.

다. 발명의 해결방법의 요지

본 발명은 정점이 되는 하나의 네트워크 장치와 상기 네트워크 장치에 접속하는 적어도 하나의 네트워크 장치로 구성되는 트리 구조 네트워크에서의 보안통신 방법에 있어서, 상기 각 네트워크 장치는 각각의 보안 개체를 구별하는 아이디를 설정하여 프레임에 추가하는 제 1과정과, 전송할 프레임의 패킷 데이터 유니트에 대하여 무결성 체크를 수행하는 제 2과정과, 상기 무결성 체크의 결과 값을 포함하는 무결성 체크 필드를 상기 전송할 프레임에 추가하는 제 3과정과, 상기 무결성 체크 필드를 포함하는 전송 프레임을 암호화하는 제 4과정과, 상기 암호화된 전송 프레임에 대한 FCS(Frame Check Sequence) 체크를 수행하는 제 5과정과, 상기 FCS 체크의 결과 값을 포함하는 FCS 필드를 상기 전송 프레임에 추가하는 과정을 포함함을 특징으로 한다.

라. 발명의 중요한 용도 EPON의 보안을 위해 사용된다.

【대표도】

도 4

【색인어】

EPON, 보안, 인증, LLID

【명세서】

【발명의 명칭】

트리 구조 네트워크 상에서의 인증과 프라이버시 보장을 위한 전송 방법{TRANSMITTING METHOD FOR AUTHENTICATION AND PRIVACY SECURITY ON TREE STRUCTURE NETWORK}

【도면의 간단한 설명】

도 1은 일반적인 PON의 구조를 도시하는 도면,

도 2는 메시지 구조의 한 예로서, 일반적인 이더넷 프레임 포맷을 도시하는 도면,

도 3은 본 발명의 실시 예에 따른 도면으로, EPON에서 암호화를 수행하는 계층을 프로토콜 스택 상에 표시한 도면,

도 4는 본 발명의 실시 예에 따른 도면으로, 암호화 기능을 수행할 수 있도록 구성된 이더넷 프레임 포맷을 도시하는 도면,

도 5는 본 발명의 실시 예에서 암호화되는 프레임 영역과 그 처리 결과에 대해 도시하는 도면.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 점대다점 구조를 가지는 트리 구조 네트워크 상에서의 보안을 보장하는 방법에 관한 것으로, 특히 이더넷 수동 광가입자망 상에서 인증과 기밀 보장을 위한 전송 방법에 관한 것이다.

<7> 정점이 되는 하나의 네트워크 장치에 접속되는 다수의 네트워크 장치가 접속되는 네트워크를 트리 구조 네트워크라 한다. 상기 점대다점 구조의 트리 구조 네트워크의 예로서, 하나의 OLT(Optical Line Termination)와 상기 OLT에 접속되는 하나 이상, 다수의 ONU(Optical Network Unit)들로 이루어지는 수동형광가입자망(Passive Optical Network; PON, 이하 "PON"이라 칭한다)을 들 수 있다.

<8> 도 1은 일반적인 PON의 구조를 도시하는 도면이다.

<9> 도 1에 도시된 바와 같이, PON은 하나의 OLT(100)와, 상기 OLT(100)에 접속되는 ONU들(110-1 내지 110-3)과 상기 ONU들(110-1 내지 110-3)에 각각 접속되는 가입자 포트(Subscriber)들(120-1 내지 120-3)로 구성될 수 있다. 상기 도 1에는 각각의 ONU들(110-1 내지 110-3)에 하나씩의 가입자(120-1 내지 120-3)가 접속된 것으로 도시되어 있으나, 실제로는 하나의 ONU(110-1 내지 110-3)에 다수의 가입자(120-1 내지 120-3)가 접속될 수 있으며, 각각의 ONU(110-1 내지 110-3)와 가입자(120-1 내지 120-3)들의 조합 또한 점대다점의 트리 구조를 가지도록 구성될 수 있다.

<10> 한편, 현재 802.3 이더넷 프레임을 점대다점의 트리 구조의 네트워크를 통해 전송하는 이더넷 수동형광가입자망(Ethernet Passive Optical Network; EPON, 이하 "EPON"이라 칭한다)에서 상향 전송의 경우 TDM(Time Division Multiplexing)방식으로 각 ONU(110-1 내지 10-3)의 데이터를 액세스하게 되고, 하향 전송의 경우에는 'Broadcast and selection' 룰을 사용한다. 즉, 하향 전송의 경우, OLT(100)로부터 임의의 특정 ONU(110-1 내지 110-3)로 전송되는 하향의 메시지는 모든 ONU들(110-1 내지 110-3)에게 전송되고, 그 중 해당되는 ONU(110-1 내지 110-3)만이 메시지를 필터링해서 받는 구조이다. 이와 같은 구조에서는 메시지를 전송 받을 ONU(110-1 내지 110-3)가 아닌 다른 ONU(110-1 내지 110-3)가 상기 데이터를 전송 받을 수 있는 가능성이 있으므로, 프라이버시를 보장받을 수 없게 된다. 즉, 보안성이 취약하다.

<11> 또한, 상향 전송의 경우에도 인증 받지 않은 ONU(110-1 내지 110-3)가 접속하거나, PON의 임의의 한 ONU(110-1 내지 110-3)가 다른 ONU(110-1 내지 110-3)인 양 위장하여 'Denial of Service' 공격을 수행하거나 자료 및 자원에 접근할 수 있다. 이러한 일들을 방지하기 위해 인증의 절차가 필요하다. 따라서, 점대다점의 트리 구조의 네트워크에서 각 ONU(110-1 내지 110-3)에 대하여 인증절차를 통한 서로 다른 키를 분배하여 메시지를 암호화하는 절차를 통하여 하향신호에 대해 프라이버시를 보장하고, 상향 전송 시의 메시지에 대한 인증을 할 수 있다.

<12> ATM PON용 암호의 기술은 이미 표준화가 완료되어 있는 상태로써 그 내용은 ITU-T G.983.1에 기술되어 있다. 그러나 이더넷 프레임을 PON이라는 피지컬 플랜트(physical plant)를 통해 전송하는 이더넷 PON의 암호기능 및 구현 방법은 현재 정의되어 있지 않다.

<13> 도 2는 메시지 구조의 한 예로서, 일반적인 이더넷 프레임 포맷을 도시하고 있다.

<14> 암호 알고리즘을 이용하여 메시지를 암호화하는데 있어 메시지의 인증을 위해 메시지뿐만 아니라 FCS(Frame Check Sequence)까지 암호화하는 방안이 제시되고 있다. 인증되지 않은 공격자(예컨대, 인증되지 않은 ONU)가 잘못된 키로 암호화하여 OLT(100)에 접속하여 메시지를 전송할 경우, 이를 OLT(100)가 인증된 키로 복호화 한 후 그 체크 비트들의 값을 비교해 보면 이 또한 FCS의 값과 틀리게 되어 FCS 체크 에러가 발생하게 되므로, 이를 통해 데이터나 데이터의 전송 근원지가 인증된 것인지 아닌지를 판단하게 된다. 그러나, 상기와 같이 FCS까지 암호화하는 경우, 링크의 결함으로 인해 링크 에러가 발생하는데 이 경우 그 암호문을 복호화한 후 그 체크 비트들의 값은 FCS의 값과 틀리게 되어 FCS 체크 에러가 발생하게 된다. 따라서, 에러가 존재하는 링크에 대해서는 FCS 체크 에러가 발생하였을 시 이 에러가 링크나 다른 디바이스 결함에 의한 에러인지, 아니면 인증되지 않은 메시지에서 오는 에러인지 구별이 불가능하게 되어 링크 관리상의 문제가 야기된다.

【발명이 이루고자 하는 기술적 과제】

<15> 따라서 상기와 같은 문제점을 해결하기 위한 본 발명의 목적은 점대다점의 트리 구조를 가지는 네트워크에서 비밀 보장을 위한 암호화 메커니즘을 포함하는 전송 방법을 제공함에 있다.

<16> 본 발명의 다른 목적은 점대다점의 트리 구조를 가지는 네트워크에서 상기 암호화된 프레임을 통해 데이터나 데이터의 전송 근원지의 인증 방법을 제공함에 있다.

<17> 본 발명의 또 다른 목적은 점대다점의 트리 구조를 가지는 네트워크인 이더넷 수동형광가입자망에서 암호화 메커니즘 및 인증을 포함하는 전송 방법을 제공함에 있다.

<18> 본 발명의 또 다른 목적은 점대다점의 트리 구조를 가지는 네트워크인 이더넷 수동형광 가입자망에서 전송 상의 보안을 위한 프레임 포맷을 제공함에 있다.

<19> 본 발명의 또 다른 목적은 점대다점의 트리 구조를 가지는 네트워크인 이더넷 수동형광 가입자망에서 전송 시 발생하는 링크 에러와 메시지 무결성을 구별함으로서 링크 관리가 가능한 암호화 방법을 제공함에 있다.

<20> 상기와 같은 목적들을 달성하기 위한 본 발명은; 정점이 되는 하나의 네트워크 장치와 상기 네트워크 장치에 접속되는 적어도 하나의 네트워크 장치로 구성되는 트리 구조 네트워크에서의 보안통신을 위한 전송방법에 있어서, 상기 각 네트워크 장치는 각각의 보안 개체를 구별하는 ID를 설정하여 프레임에 추가하는 제 1과정과, 전송할 프레임의 패킷 데이터 유니트에 대하여 무결성 체크를 수행하는 제 2과정과, 상기 무결성 체크의 결과 값을 포함하는 무결성 체크 필드를 상기 전송할 프레임에 추가하는 제 3정과, 상기 무결성 체크 필드를 포함하는 전송 프레임을 상기 보안 개체 ID에 따라 암호화하는 제 4과정과, 상기 암호화된 필드를 포함한 전송 프레임 전역에 대한 FCS(Frame Check Sequence) 체크를 수행하는 제 5과정과, 상기 FCS 체크의 결과 값을 포함하는 FCS 필드를 상기 전송 프레임에 추가하는 과정을 포함함을 특징으로 한다.

【발명의 구성 및 작용】

<21> 이하 본 발명의 바람직한 일 실시 예를 첨부한 도면을 참조하여 상세히 설명한다. 하기에서 각 도면의 구성요소들에 참조부호를 부가함에 있어서, 동일한 구성요소들에 대해서는 비

록 다른 도면상에 표시되더라도 가능한 한 동일한 부호를 가지도록 하고 있음에 유의해야 한다.

<22> 본 발명은 점대 다점의 트리 구조 네트워크에서 보안성을 높이기 위한, 인증과 프라이버시 보장을 위해 암호화하는 메커니즘에 대한 것이다. 이하 본 발명을 구체적인 실시 예를 들어 설명한다.

<23> 하기에서는 점대 다점의 트리 구조 네트워크의 대표적인 예로서, 하나의 OLT(Optical Line Terminal)(100)와 하나 이상, 다수의 ONU(Optical Network Unit)(110-1 내지 110-3)로 구성되는 PON을 예로 들어 설명하도록 한다. 하기에서 기술하는 실시 예는 PON 중에서도 특히 이더넷 PON(Ethernet Passive Optical Network)에 관한 것이다.

<24> 본 실시 예의 요지는 이더넷 프레임 내에 암호화에 대한 태그(tag)를 삽입하고, 무결성 체크(Integrity Check), 즉, 정당한 네트워크 장치가 송신한 프레임인지를 판단하기 위한 체크 필드를 삽입한 후, 메시지와 상기 IC 필드를 암호화한 후 이더넷의 MAC 계층의 기능을 수행하여 이 암호문에 대한 물리적 에러 발생 여부를 체크하는 FCS(Frame Check Sequence)를 부가하는 것이다. 하기에서는 이를 위한 절차와 메커니즘, 프레임 포맷 등을 정의한다.

<25> 도 3은 본 발명의 실시 예에 따른 도면으로, EPON에서 암호화를 수행하는 계층을 프로토콜 스택 상에 표시한 도면이다.

<26> 도 3에 도시된 바와 같이, 프로토콜 스택에는 MAC 클라이언트 계층(300-1, 300-2), MAC 제어 계층(302), MAC 계층(306), RS 계층(308), PCS(Physical Coding Sublayer, 물리 부호화 부계층, 이하 "PCS"라 칭하다) 계층(310), PMA(Physical Medium Attachment, 물리 매체 접속부, 이하 "PCS"라 칭한다) 계층(312), PMD(Physical Medium Dependent sublayer, 이하 "PMD"라

칭한다) 계층(314)이 있다. 본 발명이 수행되는 계층인 보안화 계층(304)은 MAC 클라이언트 계층(300-1, 300-2) 바로 아래 또는 MAC 제어 계층(302) 바로 아래에 위치할 수 있다.

<27> 먼저, 다수의 ONU(110-1 내지 110-3)는 등록과 인증의 절차를 거쳐 각각 다른 비밀 키(secret key)를 OLT(100)와 공유하고 있다. ONU(110-1 내지 110-3)와 OLT(100)는 비밀 마스터 키(secret master key)를 토대로 주기적으로 rekeying 절차를 통하여 가지고 있는 secret key를 새로 설정함으로서 보안성을 높일 수도 있다. 상기 절차들에 대해서는 그 설명을 생략한다.

<28> 각기 다른 키가 주어진 엔티티(entity)를 논리링크 아이디(Logical Link ID; LLID)로 구별지을 수 있다. 즉, LLID는 각 ONU(110-1 내지 110-3)들에 해당될 수 있다. 또, 하나의 ONU(110-1 내지 110-3)가 다수의 논리링크를 가지고 있을 경우, 각각의 논리링크에 해당할 수 있다. 즉, 도 1에 도시된 가입자 포트(120-1 내지 120-3)별로 LLID가 할당될 수도 있다. 즉, 인증과 키 분배가 이루어지는 단위를 LLID라 한다.

<29> 각각의 ONU(110-1 내지 110-3)나 논리링크는 서로 보관하고 있는 키를 이용하여 자신의 메시지를 암호화하게 된다. 먼저 메시지의 전송은 MAC 클라이언트 계층(300-1, 300-2)에서 트리거(trigger)되어 암호화 계층(304)으로 전송된다. 암호화 계층(304)에서는 암호화 사용/미사용(encryption enable/disable)여부에 따라 메시지에 대한 무결성 체크를 수행하여 그 결과에 대한 값인 ICV 필드를 삽입하고, 상기 ICV 필드와 메시지에 대한 암호화를 수행하고 암호 프레임 태그를 삽입하는 등의 과정을 수행한다. 이 때 암호화 프로세싱 타임으로 인해 실제 패킷이 왕복 전송을 하는데 걸리는 시간인 RTT값에 변화를 가져올 수 있다. 따라서 암호화 엔진(encryption engine)은 패킷의 길이에 무관하게 프로세싱 타임이 소요되도록 병렬 프로세싱(parallel processing)하는 것이 바람직하다. 또, 암호화 미사용 패킷(encryption-disable

packet)의 경우도 고정 라운드 트립 타입(fixed round trip time)을 보장하기 위해 암호화 프로세스와 동일한 일정 지연을 초래하도록 조정됨이 바람직하다.

<30> 도 4는 본 발명의 실시 예에 따른 도면으로, 암호화 기능을 수행할 수 있도록 구성된 이더넷 프레임 포맷을 도시하는 도면이다.

<31> 도 4에 도시된 바와 같이, 본 실시 예에 따른 이더넷 포맷은 PA(PreAmble, 프리앰블) 필드(400), DA(Destination Address, 수신지 주소) 필드(402), SA(Source Address, 송신지 주소)(404) 필드, L/Type(Length/Type, 길이 타입) 필드(406), LLID tag 필드(408), Enc tag(Encryption tag, 암호화 태그) 필드(410), PDU(Packet Data Unit) 필드(412), IC(Integrity Check) 필드(414), FCS(Frame Check Sequence) 필드(416)들로 이루어진다.

<32> LLID는 인증이나 키 배분 시 각 엔티티에 대한 식별자이다. LLID tag type을 포함하여 프레임 안에 LLID를 실어 전송할 수도 있고, 프리앰블에 넣어 전송한 후 태깅(tagging)기법으로 프레임 안에 포함되게 할 수도 있다. Enc tag 필드(410)는 프레임의 암호화의 여부를 나타낸다. 참조부호 420으로 표시된 블록은 Enc tag 필드(410)에 포함될 수 있는 것들을 보이고 있다. 상기 Enc tag 필드(410)는 암호화 태그 타입(Enc tag type)필드와 암호화 태그 정보(Enc tag info)필드로 구성될 수 있다. Enc tag info는 암호화/복호화하기 위해 필요한 정보를 가지고 있는 필드로서, 키 동기(key synchronization)나 버전 등을 포함할 수 있다. 암호화 수행 시의 어떤 모드들은 키의 시드(seed)역할을 하는 초기화 벡터(Initialization Vector; IV) 값을 필요로 하므로, Enc tag info는 이러한 IV를 포함할 수도 있다. 한편, Enc tag info를 OAM(Operation, Administration and Maintenance) 메시지나 다른 제어 메시지에 실어 전송한다면 이러한 상기 Enc tag 필드(410)는 Enc tag info 없이 태그 타입 필드로만 구성될 수 있다. Enc tag 필드(410)를 포함한 메시지는 암호화되어 있는 메시지를 의미하며, Enc tag 필

드(410)를 포함하지 않은 메시지는 암호화되어 있지 않음을 의미한다. PDU 필드(412) 이후에 PDU 필드(412)에 포함된 메시지의 무결성 체크를 위한 IC 필드(414)가 존재한다. 예컨대, 암호화 알고리즘으로서 AES(advanced Encryption standard)를 사용한 OCB 모드를 적용할 경우, IC 필드(414)는 체크 섬에 해당하는 필드로 4byte나 10 byte의 크기가 될 수 있다. 따라서 암호화 태그드 프레임, 즉, 암호화된 프레임의 경우 Enc tag 길이 + IC 길이 만큼의 프레임 길이가 부가된다. FCS 필드(416)는 링크와 MAC 계층 상에서의 에러 여부를 측정하기 위해 사용된다.

<33> MAC 클라이언트(300-1, 300-2)에서 트리거되어 암호화 계층으로 전송된 신호는 메시지와 그 외 암호화 사용/미사용 여부, 프레임 헤더(DA,SA), 에뮬레이션 계층에서 부가된 LLID tag 필드(408) 등을 포함한다.

<34> 송신할 신호에 대해 수행하는 암호화 절차는 다음과 같다.

<35> 먼저 암호화 계층(304)에서 암호화 사용/미사용 신호를 확인한다. 암호화 미사용인 메시지인 경우, 고정 라운드 트립 타임을 보장하기 위해 암호화 프로세스와 동일한 일정 지연을 초래하는 과정을 수행한다. 암호화를 사용한 메시지의 경우, 먼저 PDU 필드(412)부분에 대한 무결성 체크를 수행하여 그 값을 프레임에 첨가한다. 이러한 무결성 체크는 통상적으로 CRC(Cyclic Redundancy Check) 등의 체크 섬 등을 의미한다. 무결성 체크를 수행한 암호화 계층(304)은 LLID를 확인하여 인증 및 암호화 등에 사용하는 키를 관리하는 마스터의 레지스트리로부터 해당 LLID에 맞는 키를 가져온다. 상기 키 값을 암호 알고리즘의 input의 한 요소로 하여 PDU 필드(412)와 IC 필드(414)를 모두 암호화한다. 상기 PDU 필드(412) 앞에 암호화한 메시지로 지정된 tag type과 암호화에 대한 정보를 담은 정보 필드를 삽입하여 MAC 계층(306)

으로 전송한다. MAC 계층(306)에서는 상기 암호화 계층(304)에서 암호화한 부분을 포함한 모든 프레임 영역에 대해 FCS를 수행하여 그 값에 대한 FCS 필드(416)를 첨가한다.

<36> 한편, 수신된 메시지에 대한 암호화 절차는 다음과 같다. 통상적으로, 수신된 메시지에 대한 복호화 과정은 상기 송신 메시지에 대한 암호화 과정과 반대로 수행된다. 먼저, MAC 계층(306)으로 전송된 프레임은 암호화한 부분을 포함한 모든 프레임 영역(DA 부터 IC)(400 내지 414)에 대해 FCS를 수행하여 그 결과 값과 FCS 필드(416)의 수치를 비교한 후 그 결과를 수신상태(receive_status) 신호로 상위 계층에 전달한다. 이때 상기 수신상태 신호와 함께 FCS 필드가 제거된 프레임이 상위 계층으로 전달된다. 암호화 계층(304)에서는 MAC 계층(306)으로부터 전달받은 프레임의 LLID tag 필드(408)에서 LLID를 확인하고, Enc tag 필드(410)에서 암호화 태그 타입을 확인한다. 암호화 태그 확인 결과, 암호화 미사용의 메시지인 경우고정 라운드 트립 타입을 보장하기 위해 복호화 프로세스와 동일한 일정 지연을 초래하는 과정을 수행한다. 암호화 사용의 메지시인 경우, LLID를 확인하고 키를 관리하는 마스터의 레지스트리로부터 해당 LLID에 맞는 키를 가져온다. Enc tag 필드(410)에 포함된 encryption tag info 필드 상의 정보와 상기 마스터의 레지스트리로부터 가져온 키를 토대로 복호 알고리즘과 연계하여 PDU 필드(412)와 IC 필드(414)를 모두 복호화 한다. 이때, 해당 LLID의 키 값이 아닌 다른 값을 이용하여 암호화 또는 복호화를 수행하게 되면 복호화한 필드의 값이 원래의 값과 틀려지게 된다. 따라서, 무결성 체크 결과 값이 프레임의 IC 필드(414)의 값과 달라지게 된다. 복호화된 PDU 필드(412)에 대해 무결성 체크를 수행한 후 그 결과 값을 IC 필드(414)의 값과 비교하여 일치하지 않을 경우, 즉, 상기 메시지가 해당 LLID를 가진 인증된 근원지로부터 전송된 것이 아니라고 판단되는 경우, 메시지 무결성 브레이크 카운터에 기록한다. 일치할 경우는 암호화 타입 태그 필드를 제거한 프레임을 상위 계층으로 전송한다.

<37> 도 5는 본 발명의 실시 예에서 암호화되는 프레임 영역과 그 처리 결과에 대해 도시하고 있다.

<38> 프레임 중에서 암호화되는 영역은 DA 필드(400)에서 PDU 필드(412), IC 필드(414)까지이다. 먼저, 암호화된 DA 필드(400)~IC 필드(414) 영역의 체크 섬 값이 FCS 필드(416)의 값과 일치하여 FCS 체크를 통과할 경우는 링크나 MAC 계층의 결함으로 인한 에러가 없음을 의미한다. 이후 복호화 과정을 거쳐 복호화된 평문의 PDU 필드(412)에 대한 체크 섬 값이 IC 필드(414)의 값과 일치할 경우 올바른 키로 암호화되었다는 것을 의미하므로 이는 메시지나 메시지 전송 근원지의 무결성을 입증하는 것이 된다. 따라서, 링크 에러와 잘못된 키 암호화가 구분되는 링크 관리가 가능해 진다.

<39> 즉, 상술한 바와 같이, 본 발명에서는 점대다 네트워크에서 공유 매체를 이용하는 다른 네트워크 장치(예컨대, ONU, Subscriber 등)들에 LLID를 부여하고 해당 LLID를 이용하여 수행함으로서 각 네트워크 장치들을 구분하고 이를 구별자로 보안 통신을 수행할 수 있다. 또, 메시지의 무결성 체크 후 전송할 프레임에 IC 필드(414)를 추가하고, 상기 IC 필드(414)까지를 포함하는 프레임에 대하여 암호화를 수행한 후, 암호화된 프레임에 대하여 FCS 체크를 수행한 후 FCS 필드(416)를 추가하여 전송함으로서 메시지의 무결성 여부 판단과 링크 에러 여부 판단의 구분이 가능하게 된다.

【발명의 효과】

<40> 상술한 본 발명에 의해서 트리 구조의 네트워크에서 각각의 네트워크 모듈 단위나 이에 해당하는 논리링크에 대하여 다른 키를 부여하여 데이터를 암호화하여 전송함에 있어, 인증과 비밀 보장을 위한 암호화의 메커니즘을 정의함으로써 공유 매체 전송의 트리 구조의 네트워크

가 가지는 보안의 취약성을 보완할 수 있다. 또한 메시지 무결성과 링크 에러를 구별하여 링크 관리가 가능한 두 개의 기능을 포함하는 암호화 방법을 구현할 수 있다.

【특허청구범위】

【청구항 1】

정점이 되는 하나의 네트워크 장치와 상기 네트워크 장치에 접속되는 적어도 하나의 네트워크 장치로 구성되는 트리 구조 네트워크에서의 보안통신을 위한 전송방법에 있어서, 송신단계는

상기 각 네트워크 장치는 전송할 프레임의 패킷 데이터 유니트에 대하여 무결성 체크를 수행하는 제 1과정과,

상기 무결성 체크의 결과 값을 포함하는 무결성 체크 필드를 상기 전송할 프레임에 추가하는 제 2과정과,

상기 무결성 체크 필드를 포함하는 패킷 데이터 유니트를 암호화하는 제 3과정과,

상기 암호화된 필드를 포함한 전송 프레임 전체에 대한 FCS(Frame Check Sequence) 체크를 수행하는 제 4과정과,

상기 FCS 체크의 결과 값을 포함하는 FCS 필드를 상기 전송 프레임에 추가하는 과정을 포함함을 특징으로 하는 보안 전송방법.

【청구항 2】

제 1항에 있어서,

상기 전송단계는 송신지 네트워크 장치에 부여된 해당 논리링크 아이디를 적어도 포함하는 필드를 부가하는 과정을 더 포함함을 특징으로 하는 보안 전송방법.

【청구항 3】

제 1항에 있어서, 상기 제 3과정의 암호화는 해당 네트워크 장치의 논리링크 아이디를 적어도 포함하는 값을 이용하여 그에 해당하는 키로 암호화를 수행함을 특징으로 하는 보안 전송방법.

【청구항 4】

제 1항에 있어서, 상기 제 1과정의 무결성 체크는 체크 섬 방식으로 이루어짐을 특징으로 하는 보안 전송방법.

【청구항 5】

제 1항에 있어서, 상기 제 4과정의 FCS 체크는 체크 섬 방식으로 이루어짐을 특징으로 하는 트리 구조 네트워크에서의 전송방법.

【청구항 6】

정점이 되는 하나의 네트워크 장치와 상기 네트워크 장치에 접속되는 적어도 하나의 네트워크 장치로 구성되는 트리 구조 네트워크에서의 보안통신을 위한 전송방법에 있어서 수신단계는

상기 각 네트워크 장치는 수신한 프레임에 대한 FCS 체크를 수행하는 제 1과정과,

상기 FCS 체크를 수행한 수신 프레임의 FCS 필드를 제외하고 무결성 체크 필드를 포함하여 암호화된 패킷 데이터 유니트를 복호화하는 제 2과정과,

상기 복호화된 필드에 대하여 무결성 체크를 수행하는 제 3과정을 포함함을 특징으로 하는 보안 전송방법.

【청구항 7】

제 6항에 있어서, 상기 제 2과정의 복호화는,

수신한 프레임에 포함된, 송신지 네트워크 장치에 부여된 해당 논리링크 아이디를 적어도 포함하는 필드를 이용하여 그 해당 논리링크 아이디에 부여된 키를 이용하여 복호화하는 과정을 포함함을 특징으로 하는 보안 전송방법.

【청구항 8】

제 6항에 있어서, 상기 제 1과정의 FCS 체크는 FCS 필드를 제외한 수신 프레임의 필드들에 대한 체크 섬 값과 상기 FCS 필드의 값의 일치 여부를 판단함으로서 이루어짐을 특징으로 하는 보안 전송방법.

【청구항 9】

제 5항에 있어서, 상기 제 3과정의 무결성 체크는 패킷 데이터 유니트 필드에 대한 체크 섬 값과 무결성 체크 필드의 값의 일치여부를 판단함으로서 이루어짐을 특징으로 하는 보안 전송방법.

【청구항 10】

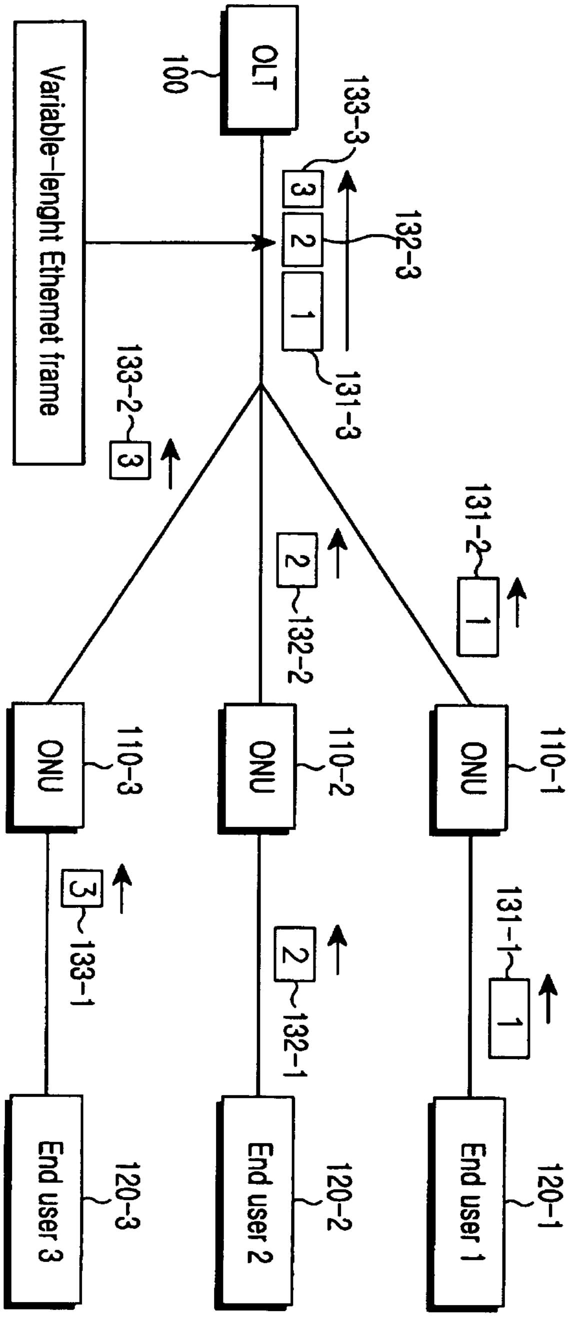
제 1항에 있어서, 이더넷 수동 광가입자 네트워크에서 상기 전송 프레임은 PA(PreAmble) 필드, DA(Destination Address) 필드(402), SA(Source Address) 필드, L/Type(Length/Type) 필드, LLID tag 필드, Enc tag(Encryption tag) 필드, PDU(Packet Data Unit) 필드, IC(Integrity Check) 필드 및 FCS(Frame Check Sequence) 필드로 구성됨을 특징으로 하는 보안 전송방법.

【청구항 11】

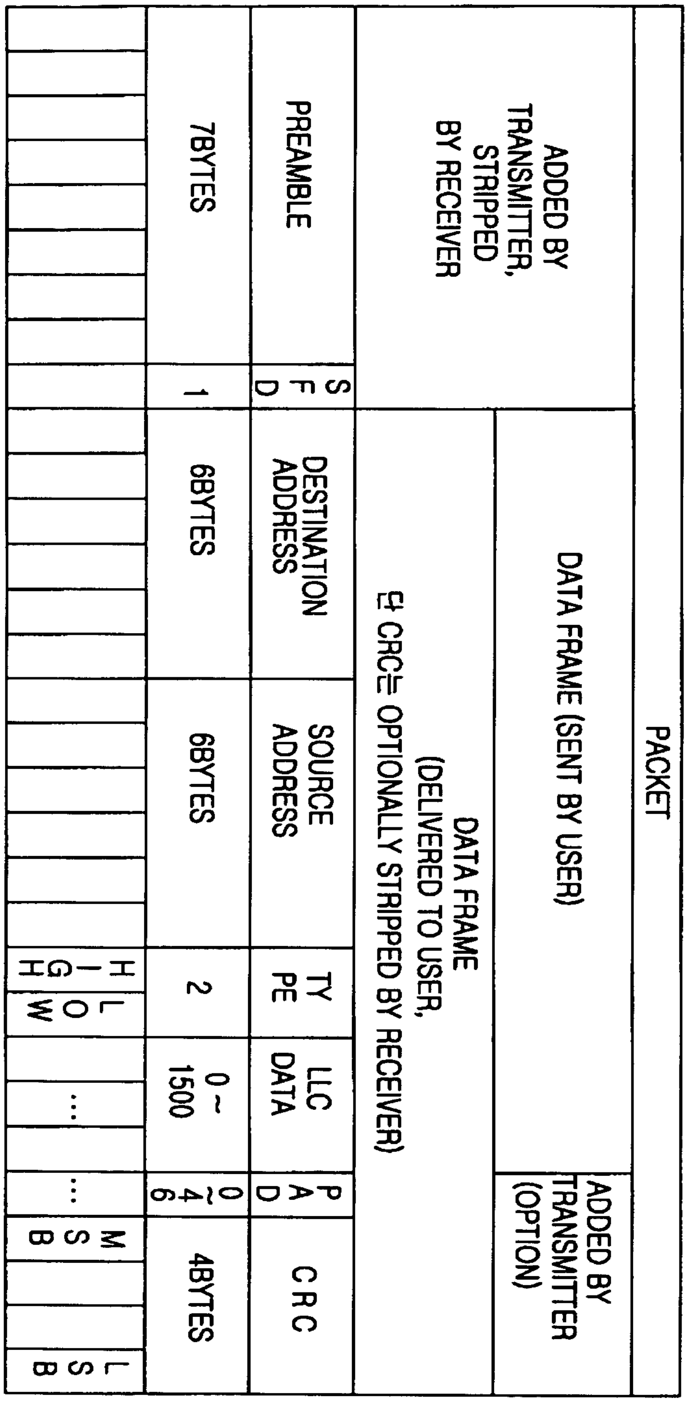
제 10항에 있어서, 상기 Enc tag 필드는 암호화 태그 타입(Enc tag type) 필드 및 암호화 태그 정보(Enc tag info) 필드로 구성됨을 특징으로 하는 보안 전송방법.

【도면】

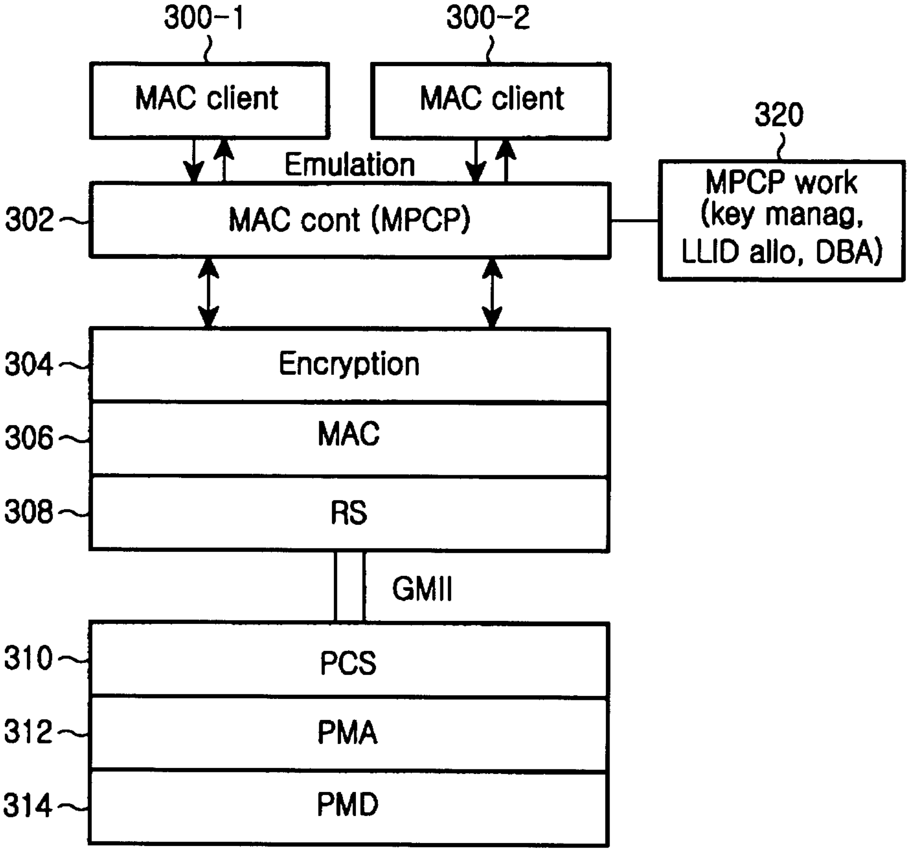
【도 1】


OLT
100
Variable-lenght Ethernet frame
133-3
132-3
131-3
3
2
1
133-2
3
2
132-2
131-2
1
ONU
110-3
ONU
110-2
ONU
110-1
3
133-1
2
132-1
131-1
1
End user 3
120-3
End user 2
120-2
End user 1
120-1

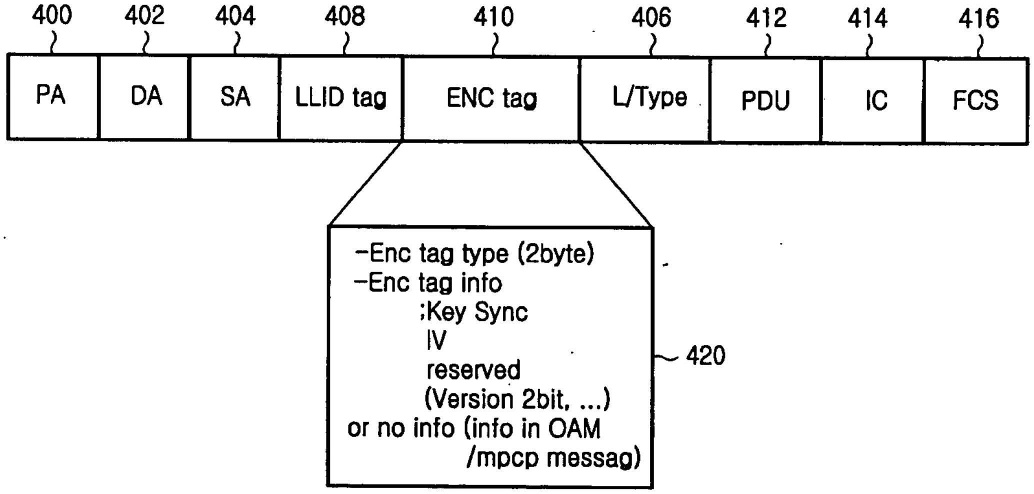
【도 2】


PACKET
ADDED BY TRANSMITTER, STRIPPED BY RECEIVER
DATA FRAME (SENT BY USER)
ADDED BY TRANSMITTER (OPTION)
DATA FRAME (DELIVERED TO USER, 단 CRC는 OPTIONALLY STRIPPED BY RECEIVER)
PREAMBLE
SFD
DESTINATION ADDRESS
SOURCE ADDRESS
TYPE
LLC DATA
PAD
CRC
7BYTES
1
6BYTES
6BYTES
2
0~1500
0~46
4BYTES
HIGH
LOW
...
...
MSB
LSB

【도 3】


300-1
MAC client
300-2
MAC client
320
MPCP work
(key manag,
LLID allo, DBA)
Emulation
302
MAC cont (MPCP)
304
Encryption
306
MAC
308
RS
GMII
310
PCS
312
PMA
314
PMD

【도 4】


400
PA
402
DA
404
SA
408
LLID tag
410
ENC tag
406
L/Type
412
PDU
414
IC
416
FCS
-Enc tag type (2byte)
-Enc tag info
;Key Sync
IV
reserved
(Version 2bit, ...)
or no info (info in OAM
/mpcp messag)
420

【도 5】